



Section II: Administrative Security
Title: Personnel Issues Related to Information Security Standard
Current Effective Date: June 30, 2008
Revision History: June 26, 2008
Original Effective Date: June 30, 2008

Purpose: To ensure that the North Carolina (NC) Department of Health and Human Services (DHHS) Divisions and Offices address issues related to personnel and information security.

STANDARD

1.0 Background

The Divisions and Offices management, with the assistance from the Division Information Security Official (ISO), shall ensure that workforce information security roles and responsibilities are clearly defined in job descriptions.

2.0 Pre-Employment Job Qualifications

All Divisions and Offices management shall be responsible for creating and updating the DHHS workforce members' information security job requirements. The Divisions and Offices management must be aware of those information security job requirements listed in the NC Office of State Personnel Manual, Section 2: Recruitment and Selection. When creating and updating information security requirements, the Divisions and Offices must abide by the DHHS information security policies and standards in conjunction with the NC DHHS Division of Human Resource (HR) – DHHS HR Policy Manual.

3.0 Defining Job Roles and Responsibilities

The Divisions and Offices management shall, to the extent possible, ensure that information security roles and responsibilities are based on separation of duties and least privileges to ensure that workforce members' security access levels are appropriately distributed.

The Divisions and Offices management shall create, document, track, and monitor information security roles and responsibilities throughout the workforce members' employment. For additional information, please refer to the NC DHHS Division of HR – DHHS HR Policy Manual.





4.0 Information Security Related to Workforce Members and Third-Party Contractors

All DHHS workforce members who have access to the state's network must comply with all state and DHHS information security policies and standards. When employing or contracting new workforce members, the Divisions and Offices management must ensure that each new workforce member complies with the NC DHHS Security Standards, Administrative Security Standards – Security Training and Awareness Standard.

All Divisions and Offices shall ensure that authorized third-party contractors (e.g., business associates, vetted employees, contractors, etc.) who have access to the state's network agree to follow governing state and DHHS policies and standards when providing services.

In order to perform the requested services, a third-party contractor may need to use the Divisions and Offices information resources and access protected information. All Divisions and Offices management must ensure that access is granted to third-party contractors only when required for performing roles and responsibilities. The DHHS business owners must approve and have full knowledge of the access rights obtained by third-party contractors.

All third-party contractors shall be fully accountable to the Divisions and Offices for any actions taken while completing their roles and responsibilities. The Divisions and Offices management must ensure that applicable DHHS policies and standards are communicated to third-party contractors.

5.0 Third-Party Contractors and Confidential Information

Confidential information must not be released to third party contractor unless applicable contract agreements (i.e., confidentiality agreements, nondisclosure agreements, etc.) have been signed by Division and Office management. Contract agreements must also specify conditions of use and security requirements.

6.0 Handling Personnel Data and/or Information

When handling personnel data and/or information, the DHHS workforce members shall adhere to the NC DHHS Security Standards, Administrative Standards – Data Stewardship Standard.

7.0 Workforce Disciplinary Actions

All Divisions and Offices shall develop and/or maintain their own policies, procedures, standards, and guidelines to handle disciplinary actions resulting from information security violations. All disciplinary actions must conform to the NC State Office of State Personnel Manual – Discipline/Appeals/and Grievances, Section 7: Employee Appeals and Grievance.





Reference:

- HIPAA Administration Simplification Act - 45 C.F.R. Parts 160 and 164.
 - HIPAA – 45 C.F.R. § 164.308(a)(1)(i) Standard: Security Management Process.
 - HIPAA – 45 C.F.R. § 164.308(a)(2) Standard: Assigned Security Responsibility.
 - HIPAA – 45 C.F.R. § 164.308(a)(3) Standard: Workforce Security.
 - HIPAA – 45 C.F.R. § 164.308(a)(4) Standard: Information Access Management.
 - HIPAA – 45 C.F.R. § 164.308(a)(5) Standard: Security Awareness and Training.
 - HIPAA – 45 C.F.R. § 164.314(a)(1) Standard: Business Associate Contracts or Other Arrangements.
- NC State Office of State Personnel Manual, Discipline/Appeals/and Grievances, Section 7: Employee Appeals and Grievance
- NC Statewide Information Technology Security Manual, Version No. 1
 - Chapter 10 – Addressing Personnel Issues Relating to Security, Section 03: Personnel Information Security Responsibilities
 - Standard – 100301 Using the Internet in an Acceptable Way
 - Standard – 100302 Keeping Passwords/PIN Numbers Confidential
 - Standard – 100303 Sharing Confidential Organization Information with Other Employees
 - Standard – 100304 Using E-mail and Postal Mail Facilities for Personal Use
 - Standard – 100305 Using Telephone Systems for Personal Reasons
 - Standard – 100306 Using the Organization’s Mobile Phones for Personal Use
 - Standard – 100307 Using Organization Credit Cards
 - Standard – 100308 Signing for Delivery of Goods
 - Standard – 100309 Signing for Work Done by Third Parties
 - Standard – 100310 Ordering Goods and Services
 - Standard – 100311 Verifying Financial Claims and Invoices
 - Standard – 100312 Approving and Authorization of Expenditures
 - Standard – 100313 Responding to Telephone Inquires
 - Standard – 100314 Sharing Confidential Information with Family Members
 - Standard – 100315 Gossip and Disclosing Information
 - Standard – 100316 Spreading Information Through the Office “Grape Vine”
 - Standard – 100317 Playing Games on Office Computers
 - Standard – 100318 Using Office Computers for Personal Use
- NC Division of Human Resource (HR)
 - DHHS HR Policy Manual
- NC DHHS Security Standards
 - Administrative Security Standards
 - Data Stewardship Security Standard
 - Security Training and Awareness Standard
- NC DHHS Policy and Procedures Manual, Section VIII – Security and Privacy, Security Manual
 - Personnel Security Policy

